AFFIDAVIT OF ANTHONY J. VENTETUOLO

I, Anthony J. Ventetuolo, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple ID **MONTANA6390@YAHOO.COM** (hereinafter the "Subject Apple ID") that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cuptertino, CA. The information to be disclosed by Apple and searched by the government is described below and in Attachments A and B.

2. I have been a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) since May 2015, and I am presently assigned to the Providence Field Office of the Boston Field Division. My responsibilities are to investigate and prevent offenses involving the unlawful use, manufacture, and possession of firearms and explosives, as well as to investigate violations of federal arson statutes. I attended and successfully completed the Department of Homeland Security, Criminal Investigator Training Program and ATF Special Agent Basic Training at the Federal Law Enforcement Training Center in Brunswick, Georgia. In August 2018, I attended and completed the ATF Firearms Interstate Nexus Training at the ATF National Center for Explosives Training and Research in Huntsville, Alabama.

3. I was previously employed by the United States Army Special Operations Command as a Training Instructor in direct support of a Special Operations military unit and completed three overseas deployments in support of the Global War on Terror. I served as a Police Officer with the City of Virginia Beach, Virginia Police Department from 2002 until

2012. I earned Bachelor of Science degrees in political science and public administration from James Madison University and a Master's degree in criminal justice from Troy University.

4. While employed as a Police Officer and Special Agent, I have investigated violations of local, state and federal criminal statutes; made arrests, prepared search and arrest warrant affidavits; interviewed defendants, witnesses and informants; and seized currency, firearms, narcotics and other evidence related to criminal investigations. I have experience and training in firearms and narcotics trafficking cases, gang investigations, arson investigations and the utilization of informants and cooperating witnesses to investigate firearms and narcotics trafficking and other organized criminal activity. I am familiar with the "street" language used by firearm and/or drug traffickers via electronic communication facilities, as well as the methods they use to disguise conversation and operations.

5. I have received training in analysis of call detail and other records from electronic communication facilities commonly used by individuals engaged in criminal activity to communicate about their illegal enterprises. I have used information obtained from communication facilities, including service provider records and GPS location information, to investigate criminal conspiracies involving firearms and narcotics offenses. In addition, I have specifically utilized the type of records that I seek in this application.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of conspiracy to distribute and

to possess with intent to distribute cocaine and other controlled substances, in violation of 21 U.S.C. § 846 (the "Subject Offense") as described in Attachment B.

PROBABLE CAUSE

8. In or about July 2018, members of the Worcester Police Department ("WPD") and ATF began investigating Junior MELENDEZ (born 1980), Juan RODRIGUEZ (born 1990), and others for unlawful firearm possession and the trafficking of powder and crack cocaine.

9. Agents[1] determined that MELENDEZ was using a cell phone assigned call number (774) 535-1317 (the "MELENDEZ Phone"). On March 13, 2019, the District Court authorized the interception of wire and electronic communications involving the MELENDEZ Phone. *See* Case No. 19-mc-94009-TSH. The District Court extended that authorization for additional thirty-day periods on April 12, 2019 and May 10, 2019.

10. Agents determined RODRIGUEZ was using a cell phone assigned call number (774) 262-0485 (the "RODRIGUEZ Phone"). On May 10, 2019, the District Court authorized the interception of wire and electronic communications involving the RODRIGUEZ Phone.

11. The investigation revealed that MELENDEZ and RODRIGUEZ worked together to obtain and distribute significant amounts of powder and crack cocaine. On June 4, 2019, RODRIGUEZ was charged by criminal complaint with conspiracy to distribute cocaine, in violation of 21 U.S.C. § 846. *See* Docket No. 19-mj-4283-DHH. A copy of the criminal complaint affidavit against RODRIGUEZ is attached here as Exhibit 1; the facts contained in that affidavit are expressly incorporated by reference herein.

[1] Unless otherwise noted, the term "agents" refers to ATF and DEA special agents, ATF task force officers, Worcester Police detectives and other law enforcement officers who participated in the investigation.

12. On June 4, 2019, this court also issued a warrant to search RODRIGUEZ's residence, 69 Cutler Street, Worcester, MA, as well as to search and seize the contents of the RODRIGUEZ Phone. *See* Case No. 19-mj-4288-DHH.

13. On June 5, ~~2020,~~ 2019 agents arrested RODRIGUEZ in Honolulu, Hawaii and seized the RODRIGUEZ Phone. ATF Digital Media Collection Specialist[2] John McKee attempted to extract the digital contents of the RODRIGUEZ Phone, which was protected with a six-digit pin code. The extraction completed by DMCS McKee confirmed the Mobile Station International Subscriber Directory Number ("MSISDN"), or phone number, for the device was (774) 262-0485; however, because of the security features of the device and the Apple iOS operating system, this extraction failed to produce any information related to the content of the phone, including Bluetooth connectivity, call logs, "chats," text messages, and device locations.[3]

14. On July 13, 2020, this court issued an order pursuant to 18 U.S.C. § 2703(c) and (d), directing Apple to disclose information about the Apple IDs associated with the RODRIGUEZ Phone. *See* Case No. 20-mj-4196. On August 12, 2020, Apple produced records in response to this order. These results confirmed two Apple IDs, jrodriguez6390@yahoo.com and the Subject Account, were associated with RODRIGUEZ and the RODRIGUEZ Phone. On August 18, 2020, this affiant requested that Apple preserve the contents of the iCloud accounts associated with these Apple IDs. Apple responded to this request on August 25, 2020. According to this response from Apple, while both the Subject Account and the

---

[2] ATF Digital Media Collection Specialists receive special training and equipment that enables them to collect digital evidence from electronic devices.

[3] Attempts to defeat the encryption of the RODRIGUEZ Phone are on-going, however, to date these attempts have been unsuccessful.

jrodriguez6390@yahoo.com are Apple IDs associated with RODRIGUEZ, only the Subject Account was linked to an iCloud account (see *infra* regarding Apple IDs and their relation to iCloud accounts and Apple devices).

15. Based on my training and experience, I am aware that Apple iCloud accounts associated with Apple devices, including Apple iPhones, often contain "back up" or duplicate files for information including, but not limited to, "Bluetooth connectivity, call logs, "chats," text messages, and device locations. I am further aware, based on my training and experience, that information related to the Bluetooth connectivity, call logs, "chats," text messages, and device locations often contain evidence of the commission of the Subject Offense. Information about Bluetooth connectivity and GPS location can establish the device's presence at certain times and places, while information related to SMS messages, "chats" and call logs can provide information about the nature of communication about illicit activity.

INFORMATION REGARDING APPLE ID AND iCLOUD[4]

16. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

[4] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

17. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain

enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

18. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

19. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to

access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

20. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

21. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

22. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

23. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps

may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

SUMMARY OF PROBABLE CAUSE

24. This matter concerns firearms and the distribution of controlled substances by MELENDEZ, RODRIGUEZ and others. I know based on my training and experience that individuals who illegally possess, distribute and use controlled substances and firearms generally communicate with other individuals, including co-conspirators, in order to further their criminal activity. In my training and experience, such individuals will communicate using SMS and MMS messages, photographs, screenshots from websites and other URLs.

25. I know based on this investigation that RODRIGUEZ used his cell phone as part of his criminal activities. This includes the numerous phone calls and text messages related to the distribution of cocaine that were intercepted over a three-month period (see Exhibit 1, ¶¶ 15-16, 18, 37-38, 63). Those calls included a suggestion that RODRIGUEZ communicated to MELENDEZ through a means not subject to interception by law enforcement. Exhibit 1, ¶ 69 n.9). The investigation also included a judicially authorized search of the MELENDEZ Phone during this investigation. *See* 18-mj-4434-DHH. That search revealed that while RODRIGUEZ and MELENDEZ communicated via wire and electronic communications subject to intercept under the aforementioned District Court authorizations, and also communicated via iMessage, FaceTime calls and other messenger applications. This creates probable cause to believe that many of the features of RODRIGUEZ's iCloud account will contain evidence of the Subject Offense.

26. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

27. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or

services used to communicate with co-conspirators. In addition, emails, SMS and MMS messages, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

30. In addition, GPS information may show where RODRIGUEZ committed acts in furtherance of his crimes, where witnesses or co-conspirators are located of where evidence is stored.

31. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the Subject Offense.

32. Based on the foregoing information, I conclude that there is likely information, including communications and location information pertinent to the Subject Offense stored in the iCloud account associated with the Subject Apple ID.

33. This conclusion is based on information obtained through this investigation, including the court-authorized interception of electronic and wire communications over the MELENDEZ and RODRIGUEZ Phones, as well as the information produced by Apple confirming the iCloud account under the Subject Apple ID was associated with the RODRIGUEZ Phone. Furthermore, based on the unsuccessful attempt to fully execute the warrant authorizing the search of the RODRIGUEZ Phone, it is likely the iCloud account associated with the RODRIGUEZ Phone will contain information previously unavailable to the government.

34. Moreover, given the features of the Apple iCloud, and Apple ID described above, as well as the fact that RODRIGUEZ used the Subject Apple ID in connection with the

RODRIGUEZ Phone, it is likely that a search of the iCloud account associated with the Subject Apple ID could produce evidence related to the Subject Offense even if RODRIGUEZ deleted this evidence from his device prior to the searches conducted of them.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

[REMAINDER OF PAGE LEFT BLANK]

CONCLUSION

36. Based on the foregoing, I request that the Court issue the proposed search warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

38. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Anthony J Ventetuolo
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1

on October 6, 2020: 5:04 p.m.

David H. Hennessy
United States Magistrate Judge